

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



550 989

(43) Internationales Veröffentlichungsdatum
7. Oktober 2004 (07.10.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/086157 A1

(51) Internationale Patentklassifikation⁷: G05B 19/042, B60G 17/015

(21) Internationales Aktenzeichen: PCT/EP2004/050217

(22) Internationales Anmeldedatum:
27. Februar 2004 (27.02.2004)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
103 13 409.3 25. März 2003 (25.03.2003) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): CONTINENTAL TEVES AG & CO. OHG [DE/DE]; Guerickestrasse 7, 60488 Frankfurt (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): KOHL, Andreas [DE/DE]; Am Obstmarkt 34, 55126 Mainz (DE). KEBBEL, Christian [DE/DE]; Schenkstrasse 12, 60489 Frankfurt (DE).

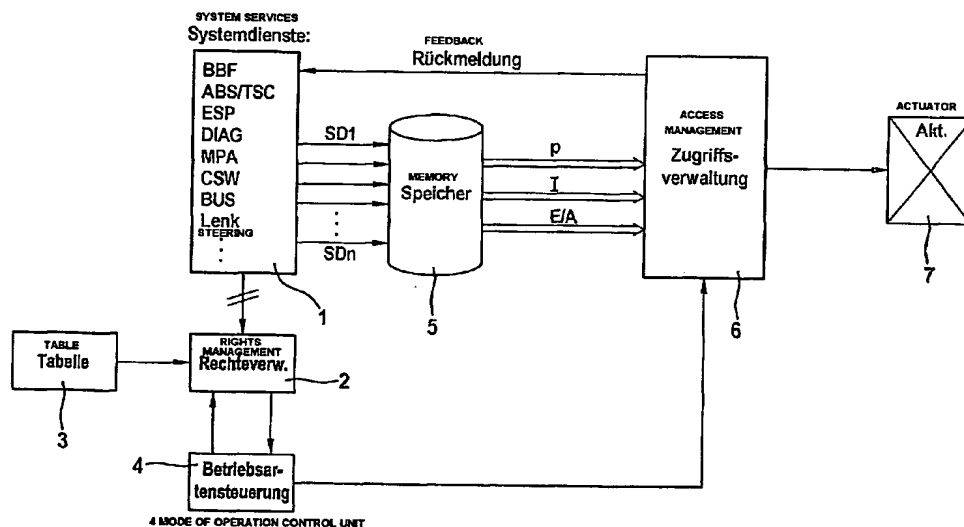
(74) Gemeinsamer Vertreter: CONTINENTAL TEVES AG & CO. OHG; Guerickestrasse 7, 60488 Frankfurt (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR THE PREVENTION OF ERRONEOUS ACTUATOR ACCESS IN A MULTIFUNCTIONAL GENERAL ELECTRONIC CONTROL SYSTEM

(54) Bezeichnung: VERFAHREN ZUM VERMEIDEN VON FEHLERHAFTEN AKTUATORZUGRIFFEN IN EINEM MULTIFUNKTIONALEN ELEKTRONISCHEN GESAMTREGELUNGSSYSTEM



(57) Abstract: Disclosed is a method for preventing erroneous actuator access in a multifunctional general electronic control system in which the actuator access requirements emanate from different system services (1). According to said method, a rights management (2) which detects the authorization of actuator access requirements, a mode of operation control unit (4), and an access management (6) are integrated into the general control system. The rights management (2) causes the mode of operation to be set or modified according to predefined rules when a system service (1) requests access by taking into account the actual mode of operation of the general system and reports the current mode of operation to the access management (6). The access management (5) authorizes actuation of the actuator by the authorized system service (1) in accordance with the reported general mode of operation while the actuator access requirements of the system services (1) are processed according to predefined arbitration rules.

[Fortsetzung auf der nächsten Seite]

WO 2004/086157 A1



TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) **Zusammenfassung:** Bei einem Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenartigen Systemdiensten (1) ausgehen, wird in die das Gesamtregelungssystem eine Rechteverwaltung (2), Berechtigung von Aktuatorzugriffsanforderungen feststellt, eine Betriebsartensteuerung (4) und eine Zugriffsverwaltung (6) integriert. Die Rechteverwaltung (2) führt bei einer Zugriffsanforderung durch einen Systemdienst (1) unter Berücksichtigung der momentanen Betriebsart des Gesamtsystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbei und meldet die aktuelle Betriebsart der Zugriffsverwaltung (6). Von der Zugriffsverwaltung (5) werden in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung durch den "berechtigten" Systemdienst (1) zugelassen und die Aktuatorzugriffsanforderungen der Systemdienste (1) nach vorgegebenen Arbitrationsregeln verarbeitet.

**Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen
in einem multifunktionalen elektronischen Gesamtregelungs-
system**

Die Erfindung bezieht sich auf ein Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenartigen Systemdiensten ausgehen. Das Verfahren ist insbesondere für Fahrzeugregelungssysteme geeignet.

Es sind bereits komplexe Kraftfahrzeugregelungssysteme bekannt, die mehrere Funktionen, wie Antiblockierschutz (ABS), Anfahrtschlupfregelung (ASR), Fahrstabilitätsregelung (ESP), elektrische Überlagerungslenkung, Bremsassistent, System- oder Komponentendiagnose usw. vereinen. Es besteht der Wunsch, diese und weitere Funktionen und Hilfsfunktionen, wie Überwachung, Fehlersignalisierung, Reifendrucküberwachung etc., ebenfalls mit Hilfe eines gemeinsamen elektronischen Systems zu steuern. Die verschiedenen Funktionen und Hilfsfunktionen werden dabei zum großen Teil mit Hilfe derselben Aktuatoren, wie Druckregelventilen, Hydraulikpumpen, Warnlampen etc., ausgeführt oder vorbereitet. Die Zugriffe zu den einzelnen Aktuatoren können dabei durchaus gleichzeitig erfolgen. Dies führt verständlicher Weise zu Konflikten. Ein Zugriff zu einem Aktuator durch ein Regelungssystem oder einen Regelungsbefehl untergeordneter Bedeutung anstelle eines z.B. aus Sicherheitsgründen momentan wichtigeren Befehls muss verhindert werden.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde sicherzustellen, dass in einem komplexen System der vorgenannten Art bei konkurrierenden Aktuatorzugriffsanforderun-

- 2 -

gen kein "fehlerhafter" , nicht berechtigter Zugriff zu einem Aktuator erfolgt. "fehlerhaft" ist dabei ein Zugriff durch eine Anforderung, die momentan unerwünscht ist, weil eine Arbitrierungsart gefordert wird, die in der aktuellen Betriebsphase nicht zulässig ist (z.B. eine Diagnosemaßnahme während der Fahrt) oder aus zahlreichen anderen Gründen.

Es hat sich herausgestellt, dass diese Aufgabe durch das im Anspruch 1 beschriebene Verfahren gelöst werden kann, dessen Besonderheit darin besteht, dass in das System eine Rechteverwaltung, die bei einer Aktuatorzugriffsanforderung die Berechtigung des Systemdienstes zur Änderung der momentanen Betriebsart des Gesamtregelungssystems feststellt, eine Betriebsartensteuerung und eine Zugriffsverwaltung eingefügt werden, dass die Rechteverwaltung bei einer Zugriffsanforderung durch einen Systemdienst unter Berücksichtigung der momentanen Gesamtbetriebsart des Gesamtregelungssystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbeiführt und die aktuelle Betriebsart der Zugriffsverwaltung meldet, und dass die Zugriffsverwaltung in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung nur durch den "berechtigten" Systemdienst zulässt und die Aktuatorzugriffsanforderungen der Systemdienste nach vorgegebenen Arbitrationsregeln verarbeitet.

Erfindungsgemäß wird also in das elektronische Steuersystem eines multifunktionalen Gesamtregelungssystems eine zusätzliche Rechte- und Zugriffsverwaltung integriert, die dazu führt, dass nur die in der jeweiligen Betriebsart "erwünschten", festen vorgegebenen Regeln entsprechende Zugriffsanforderungen der verschiedenen oder verschiedenartigem Systemdienste zum Aktuator durchgelassen werden. Den z.B. aus Sicherheitsgründen vorzuziehenden Aktionen wird von der Zugriffsverwaltung Vorrang oder Priorität eingeräumt.

- 3 -

Durch die erfindungsgemäße Rechte- und Zugriffsverwaltung wird es möglich, Basisfunktionen und Hilfs- oder Fremdfunktionen in einem System zu integrieren, ohne die Basisfunktionen zu gefährden. Durch die Rechte- und Zugriffsverwaltung wird verhindert, dass z.B. durch einen "fehlerhaften", nicht berechtigten Zugriff auf einen Aktuator eine Bremsbetätigungsanforderung, die aus Sicherheitsgründen Vorrang haben muss, nicht mehr durchgeschaltet werden kann. Die Erfindung macht es also erst möglich, dass zahlreiche wichtigere und - je nach Situation bzw. Betriebsart - weniger wichtige Funktionen integriert werden können.

Nach einem vorteilhaften Ausführungsbeispiel des erfindungsgemäßen Verfahrens werden die Aktuatorzugriffsanforderungen der Systemdienste in einem Speicher erfasst und nach Arbitrationsarten getrennt zur Zugriffsverwaltung weitergeleitet.

Eine besonders vorteilhafte Ausführungsart der Erfindung besteht, dass die zu einem Aktuator durchgelassene, von einem Systemdienst ausgehende Aktuatorzugriffsanforderung durch zweistufige Arbitration, nämlich durch eine "vertikale" und eine "horizontale" Arbitration, bestimmt wird.

Nach einem weiteren Ausführungsbeispiel der Erfindung werden in der Zugriffsverwaltung in einem ersten Schritt die nicht berechtigten Zugriffsanforderungen in Abhängigkeit von der gemeldeten, aktuellen Gesamtbetriebsart ermittelt, eliminiert oder zurückgewiesen werden. In einem zweiten Schritt wird durch vertikale Arbitration eine Bewertung und Auswahl der berechtigten Zugriffsanforderungen nach vorgegebener Rangfolge der Arbitrationsarten durchgeführt, wobei einem "Stromsignal" höhere Priorität als einem "Drucksignal" und einem "EIN/AUS-Signal" höhere Priorität als einem Stromsig-

- 4 -

nal zugemessen werden. Schließlich erfolgt in einem dritten Schritt durch horizontale Arbitration eine Bewertung und Auswahl der in dem zweiten Schritt ermittelten Zugriffsanforderungen nach Priorität des Signals, mit dem der ausgewählte Systemdienst den Aktuator ansteuern will.

Es ist zweckmäßig, die Rechte der Systemdienste zur Änderung der Betriebsart in einem Festwertspeicher, auf den die Rechteverwaltung Zugriff hat, z.B. in Form einer Tabelle, festzuhalten.

Wird das erfindungsgemäße Verfahren bei einem Gesamtregelungssystem für Kraftfahrzeuge angewendet, das als Basissystem eine Bremsanlage (EHB, EMB) enthält, werden als Systemdienste, von denen Aktuatorzugriffsanforderungen ausgehen, die Basisbremsfunktionen (BBF), Radschlupfregelungsfunktionen (wie ABS, ASR(TCS), ESP), Diagnosefunktionen (DIAG), Motorpumpenregelungssysteme (MPA) und Schnittstellen (BUS) erfasst und durch die Rechteverwaltung in Verbindung mit der Zugriffsverwaltung kontrolliert.

Es können noch weitere Systemdienste, wie "Fremdsoftware", (CSW) "Lenkungenfunktionen" (Lenk) etc., in das Gesamtsystem integriert werden.

Bei einem Gesamtregelungssystem für Kraftfahrzeuge wird vorteilhafter Weise in der Betriebsartensteuerung zumindest zwischen den Betriebsarten "Normalbetrieb", der sich nach Beendigung der Startphase beim Ausbleiben einer Fehlermeldung einstellt, der Betriebsart "Startphase", die z.B. bis zum Ablauf einer vorgegebenen Zeitspanne, bis zum erstmaligem Erreichen einer Mindestgeschwindigkeit und/oder bis zum Abschluss von anfänglichen Prüfroutinen gilt, der Betriebsart "Diagnose", der Betriebsart "Fremdsoftware", die bei einer

- 5 -

Aktuatorzugriffsanforderung durch ein Fremd- oder Hilfssystem ausgelöst wird, und der Betriebsart "Failsafe", die auf das Vorliegen einer Fehlermeldung hinweist, unterschieden.

Weitere Merkmale, Vorteile und Anwendungsmöglichkeiten der Erfindung gehen aus der folgenden Beschreibung von Einzelheiten eines Ausführungsbeispiels anhand der beigefügten Zeichnung hervor. Es zeigen

Fig. 1 in schematischer Darstellung Funktionselemente eines elektronischen Gesamtregelungssystems zur Ausführung des erfindungsgemäßen Verfahrens und

Fig. 2 ebenfalls in schematischer Darstellung einen Teil des Gesamtregelungssystems nach Fig. 1 zur Veranschaulichung der Funktionsweise der Zugriffsverwaltung.

Das im folgenden als vereinfachtes Beispiel beschriebene Gesamtregelungssystem ist für ein Kraftfahrzeug mit einer komplexen Bremsanlage, wie einem elektrohydraulischen Bremsensystem (EHB) vorgesehen, das mit Systemen und Funktionen unterschiedlicher Art, wie Bremsassistent, Geschwindigkeits- oder Abstandregelungssystemen, Diagnosesystemen, Lenksystemen (z.B. Überlagerungslenkung) etc. zusammenarbeiten kann. Das Bremsensystem, einschließlich der zugehörigen Regulationssysteme und -funktionen ABS, ASR, ESP etc. wird als Basis-system betrachtet, die übrigen Systeme oder Funktionen als Fremd- oder Hilfssysteme.

In Fig. 1 werden die Dienste, von denen Aktuatorzugriffsanforderungen ausgehen, die nach dem erfindungsgemäßen Verfahren "verwaltet", d.h. auf ihre Berechtigung geprüft werden, durch einen Funktionsblock 1 symbolisch dargestellt. In dem hier beschriebenen Ausführungsbeispiel nach der Erfindung

- 6 -

handelt es sich, wie in 1 angedeutet, im wesentlichen um die folgende Dienste:

- BBF bezeichnet die Basisbremsfunktion, die z.B. bei Brake-By-Wire-Systemen (EHB; EMB) auch in Standardsituationen elektronische Steuerung verlangt;
- ABS, ASR(TCS), ESP sind unter diesen Abkürzungen bekannte Regelungsfunktionen;
- DIAG bezeichnet Diagnosefunktionen;
- MPA ist die Bezeichnung für ein Motorpumpenaggregat, vom dem ebenfalls Aktuatorzugriffsanforderungen ausgehen;
- CSW symbolisiert Fremd- oder Hilfssysteme (CSW = Customer Software);
- BUS bezeichnet eine Schnittstelle, wie CAN-Bus, über die u.a. auch Zugriffsanforderungen von Zubehörfunktionen oder von Fremdsystemen (CSW) geleitet werden;
- Lenk bezeichnet Lenksysteme, wie Überlagerungslenkungen.

Zugriffsanforderungen von Abstandsregelungssystemen (ACC), Geschwindigkeitsregelungssystemen (Tempomat) etc. können ebenfalls über den Systemdienst "BUS", über die Schnittstelle CSW oder über einen weiteren Systemdienst mit eigener Identität (ID) in das Gesamtregelungssystem integriert werden.

Die von den Systemdiensten 1 ausgehenden Aktuatorzugriffsanforderungen werden in einer Rechteverwaltung 2 auf Zulässigkeit oder Berechtigung in der aktuellen Situation, d.h. in der momentanen Betriebsart (Gesamtbetriebsart), überprüft. Hierzu dient eine Rückmeldung aus einer Betriebsartensteuerung 3.

Jeder Dienst wird durch seine ID eindeutig erkannt. Als Betriebsarten, die unterschiedliche Reaktionen verlangen, sind beispielsweise die folgenden von Bedeutung:

- 7 -

"Normal"	"Normal-Betrieb" ist z.B. nach längerer Betriebszeit eines Kraftfahrzeugs ohne Fehlermeldung gegeben;
"Start-Phase"	gilt z.B. solange die einzelnen Systeme noch nicht voll in Funktion sind oder Routineüberprüfungen noch nicht abgeschlossen sind;
"Diagnose"	diese Betriebsart herrscht z.B. in der Werkstatt oder in der Startphase des KFZ während des Ablaufs von Prüfroutinen;
"CSW"	Fremdsoftware: diese Betriebsart wird z.B. eingestellt, wenn die ID des den Zugriff anfordernden Systemdienstes erkennen lässt, dass die Anforderung nicht von einer Basisfunktion, sondern von einer Zubehör- bzw. Hilfsfunktion oder "Fremdfunktion" stammt;
"Failsafe"	im System wurde ein Fehler erkannt, der Betriebseinschränkungen zur Folge hat.

Die Regeln zur Beurteilung der "Berechtigung" in Abhängigkeit von dem identifizierten Systemdienst und von der aktuellen Betriebsart (Gesamtbetriebsart) sind fest vorgegeben. Die Regeln sind, wie Fig. 1 zeigt, in dem beschriebenen Ausführungsbeispiel der Erfindung in einem Festwertspeicher 3, z.B. tabellarisch, festgehalten.

Die Zugriffsanforderung des jeweiligen Systemdienstes 1 wird von der Rechteverwaltung 2 sofort abgelehnt oder ignoriert, wenn in der aktuellen Gesamtbetriebsart keine Berechtigung zu der Aktuatorzugriffsanforderung gegeben ist. Wenn die Anforderung in der aktuellen Betriebsart "berechtigt" ist, wird durch die Betriebsartensteuerung 4, falls erforderlich, ein Wechsel der Betriebsart des Gesamtregelungssystems herbeigeführt. Die aktuelle Betriebsart wird einer Zugriffsver-

- 8 -

waltung 6 gemeldet; außerdem erfolgt eine Rückmeldung an die Rechteverwaltung 2.

Die Aktuatorzugriffsanforderungen der einzelnen Systemdienste 1 werden über die Signalwege SD1 bis SDn, gleichzeitig mit der Rechteüberprüfung in der Rechteverwaltung 2, über einen Zwischenspeicher 5 der Zugriffsverwaltung 6 zugeführt, die nach vorgegebenen Regeln durch Arbitration gesteuert festlegt, welche Aktuatorzugriffsanforderung der Systemdienste 1 in der aktuellen Betriebsart tatsächlich bis zu einen Aktuator 7 durchgelassen wird. Alle anderen Anforderungen werden ignoriert oder wegen "fehlender Berechtigung" zurückgewiesen; die Akzeptanz und/oder die "Ablehnung" der Anforderung wird den Systemdiensten 1 zurückgemeldet.

Wie Fig. 2 veranschaulicht, werden in dem Zwischenspeicher 5 die Aktuatorzugriffsanforderungen nach Arbitrationsarten, d.h. nach Signalen gleicher physikalischer Einheit (hier: Druck "p", Strom "I" oder EIN/AUS-Signal "E/A"), sortiert und zur Zugriffsverwaltung weitergeleitet.

In der Zugriffsverwaltung 6 werden in einem ersten Schritt die in der aktuellen Gesamtbetriebsart "nicht berechtigten" Anforderungen zurückgewiesen oder eliminiert. Sodann findet eine zweistufige Arbitration der verbliebenen Aktuatorzugriffsanforderungen statt. In einer ersten Stufe, symbolisiert durch einen Block 8 in Fig. 2, werden die "berechtigten" Anforderungen nach vorgegebener Rangfolge oder Prioritätsrang der einzelnen Arbitrationsarten bewertet; dies wird als "vertikale" Arbitration bezeichnet.

Anschließend wird in einem zweiten Schritt oder einer zweiten Stufe 9 durch "horizontale" Arbitration eine Bewertung der verbleibenden Anforderungen gleicher Arbitrationsart ge-

- 9 -

troffen und festgelegt, welche der Aktuatorzugriffsanforderungen tatsächlich bis zu dem Aktuator 7 durchgelassen wird. Symbolisiert durch einen Umschalter 10 wird das Ausgangssignal der Stufe 9 - je nach Arbitrationsart, d.h. hier "Druck", "Strom" oder "EIN/AUS"-Signal - direkt oder nach Weiterverarbeitung in einem Druckregler 11 und/oder in einem Stromregler 12 zu dem Aktuator 6 weitergeleitet. 9

In dem hier beschriebenen Ausführungsbeispiel der Erfindung ist der Aktuator 7 eine Spule, z.B. die Ventilschule eines Bremsdrucksteuerventils. Ein Befehl oder Signal der Einheit oder Dimension "EIN/AUS" führt unmittelbar zur Reaktion des Ventils. Dem "EIN/AUS"-Signal wird daher im Sinne der horizontalen Arbitration die "höchste" Priorität eingeräumt. Ein Signal der Einheit oder Dimension "Strom" muss dagegen zunächst in einem Stromregler 12 (siehe Fig. 2) ausgewertet und in einen "EIN/AUS"-Befehl umgewandelt werden. Eine Druckänderungsanforderung, also ein Signal der Dimension "Druck", muss zunächst in einem Druckregler 11 in eine Stromänderungsanforderung und danach mit Hilfe des Stromreglers 12 in ein Aktuatorbetätigungssignal bzw. in ein "EIN/AUS"-Signal gewandelt werden. Ein Signals der Dimension "Strom" genießt daher im vorliegenden Ausführungsbeispiel eine höhere Priorität als ein Signal der Dimension "Druck". Bei konkurrierenden Signalen der Dimension "Druck", "Strom" und "EIN/AUS" gelangt das E/A-Signal zur Ausführung; fehlt ein E/A-Signal, wird das Strom-Signal vorgezogen.

Die Zugriffsverwaltung 6 selektiert die Aktuatorzugriffsanforderungen nach vorgegebenen Regeln in Abhängigkeit von der aktuellen Betriebsart. Beispielsweise sind in der Betriebsart "Normal" nur Druck-Sollwertanforderungen "rechtmäßig" und werden ausgewertet; andere Anforderungen werden von der Zugriffsverwaltung 6 zurückgewiesen oder ignoriert. In der

- 10 -

Betriebsart "Fremdsoftware" (CSW) sind nur Stellbefehle bzw. Aktuatorzugriffsanforderungen in Form von Drucksignalen erlaubt. In der Betriebsart "Diagnose" sind Stellbefehle in Form von Stromsignalen oder Ventil-Schaltbefehlen, nicht jedoch von Drucksignalen zulässig. In der Betriebsart "Failsafe" sind nur Aktuatoranforderungen, die von dem Kernsystem ausgehen, zu dem vor allem die sicherheitskritischen Systemdienste gehören, nicht jedoch Aktuatoranforderungen von Zubehörssystemen, Hilfssystemen oder Fremdsystemen (CSW) "rechtmäßig".

Dies sind nur relativ einfache Beispiele. Eine Vielzahl weiterer Vorgaben lässt sich mit Hilfe der Zugriffsverwaltung 6 in Verbindung mit der Rechteverwaltung 2 (3) realisieren.

- 11 -

Patentansprüche:

1. Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenen oder verschiedenartigen Systemdiensten (1) ausgehen, dadurch **gekennzeichnet**, dass in das System eine Rechteverwaltung (2), die bei einer Aktuatorzugriffsanforderung die Berechtigung des Systemdienstes (1) zur Änderung der momentanen Betriebsart des Gesamtregelungssystems feststellt, eine Betriebsartensteuerung (4) und eine Zugriffsverwaltung (6) eingefügt werden, dass die Rechteverwaltung (2) bei einer Zugriffsanforderung durch einen Systemdienst (1) unter Berücksichtigung der momentanen Gesamtbetriebsart des Gesamtregelungssystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbeiführt und die aktuelle Betriebsart der Zugriffsverwaltung (6) meldet, und dass die Zugriffsverwaltung (6) in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung nur durch den "berechtigten" Systemdienst (1) zulässt und die Aktuatorzugriffsanforderungen der Systemdienste (1) nach vorgegebenen Arbitrationsregeln verarbeitet.
2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, dass die Aktuatorzugriffsanforderungen der Systemdienste (1) in einem Speicher (5) erfasst und nach Arbitrationsarten sortiert zur Zugriffsverwaltung (6) weitergeleitet werden.
3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, dass die zu einem Aktuator (7) durchgelassene, von einem Systemdienst (1) ausgehende Aktuatorzugriffsan-

- 12 -

forderung durch zweistufige Arbitration, nämlich durch eine "vertikale" und eine "horizontale" Arbitration, bestimmt wird.

4. Verfahren nach einem oder mehreren der Ansprüche 1 bis 3 2, dadurch **gekennzeichnet**, dass in der Zugriffsverwaltung (6) in einem ersten Schritt die nicht berechtigten Zugriffsanforderungen in Abhängigkeit von der gemeldeten, aktuellen Gesamtbetriebsart ermittelt, eliminiert oder zurückgewiesen werden, dass in einem zweiten Schritt durch vertikale Arbitration eine Bewertung und Auswahl der berechtigten Zugriffsanforderungen nach vorgegebener Rangfolge der Arbitrationsarten durchgeführt wird, wobei einem "Stromsignal" höhere Priorität als einem "Drucksignal" und einem "EIN/AUS-Signal" höhere Priorität als einem "Stromsignal" zugemessen wird, und dass in einem dritten Schritt durch horizontale Arbitration eine Bewertung und Auswahl der in dem zweiten Schritt ermittelten Zugriffsanforderungen nach Priorität des Signals für die Ansteuerung des Aktuators (7) erfolgt.
5. Verfahren nach einem oder mehreren der Ansprüche 1 bis 4, dadurch **gekennzeichnet**, dass die Rechte der Betriebsdienste (1) zur Änderung der Betriebsart in einem Festwertspeicher (3), auf den die Rechteverwaltung (2) Zugriff hat, festgehalten werden.
6. Verfahren nach einem oder mehreren der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, dass bei einem Gesamtregelungssystem für Kraftfahrzeuge, das als Basissystem eine Bremsanlage (EHB, EMB) enthält, als Systemdienste (1), von denen die Aktuatorzugriffsanforderungen ausgehen, die Basisbremsfunktionen (BBF), Radschlupfregelungs-

- 13 -

funktionen (wie ABS, ASR(TCS),ESP), Diagnosefunktionen (Diag), Motorpumpenregelungssysteme (MPA) und Schnittstellen (BUS) erfasst und durch die Rechteverwaltung (2) in Verbindung mit der Zugriffsverwaltung (5) kontrolliert werden.

7. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass weitere Systemdienste (1), wie "Fremdsoftware" (CWS), "Lenkungenfunktionen" (Lenk), etc. in das Gesamtsystem integriert werden.
8. Verfahren nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass bei einem Gesamtregelungssystem für Kraftfahrzeuge in der Betriebsartensteuerung (3) zumindest zwischen den Betriebsarten "Normalbetrieb", der sich nach Beendigung der Startphase beim Ausbleiben einer Fehlermeldung einstellt, der Betriebsart "Startphase", die z.B. bis zum Ablauf einer vorgegebenen Zeitspanne, bis zum erstmaligem Erreichen einer Mindestgeschwindigkeit und/oder bis zum Abschluss von anfänglichen Prüfroutinen gilt, der Betriebsart "Diagnose", der Betriebsart "Fremdsoftware", die bei einer Aktuatorzugriffsanforderung durch ein Fremd- oder Hilfssystem ausgelöst wird, und der Betriebsart "Fail-safe", die auf das Vorliegen einer Fehlermeldung hinweist, unterschieden wird.

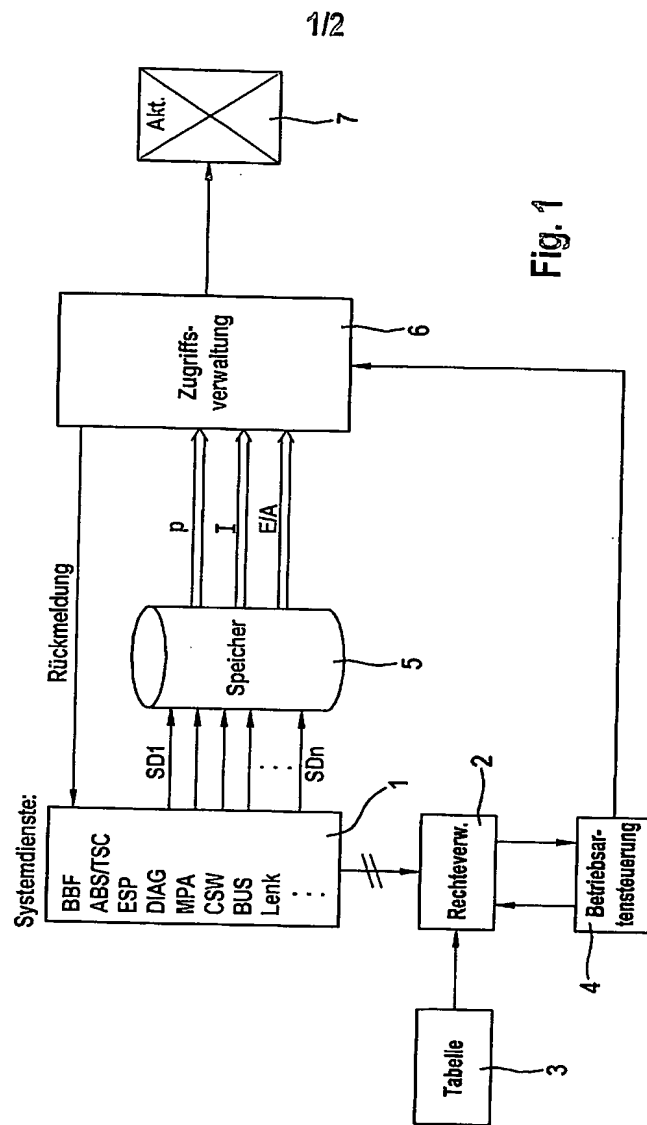


Fig. 1

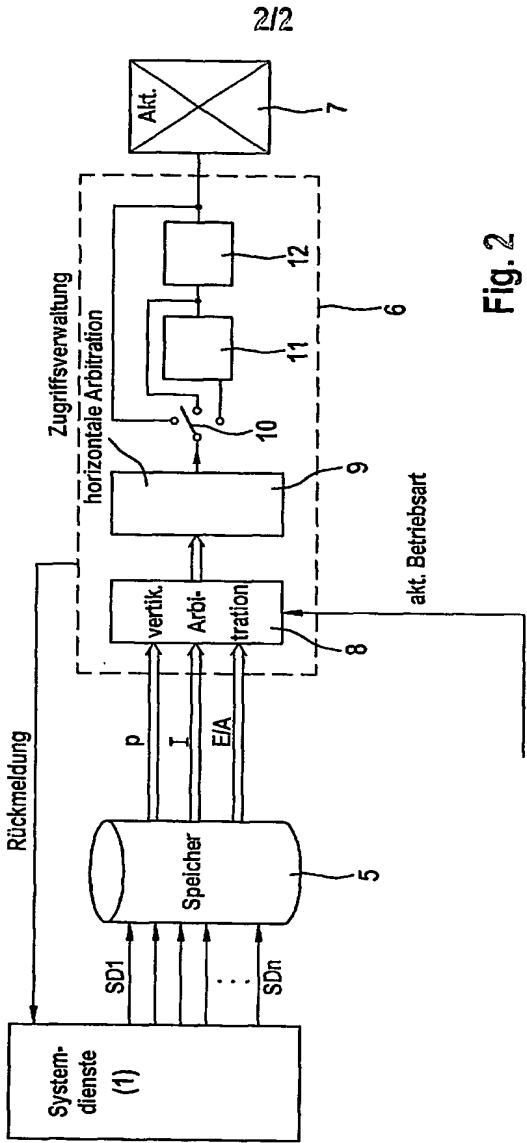


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050217

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G05B19/042 B60G17/015

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G05B B60G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 100 25 493 A (DAIMLER CHRYSLER AG) 6 December 2001 (2001-12-06) paragraphs '0002! - '0022! paragraphs '0042! - '0050! figure 1	1-8
A	DE 197 04 841 A (ITT MFG ENTERPRISES INC) 13 August 1998 (1998-08-13) column 2, line 19 - line 25 column 2, line 46 - column 3, line 19 column 3, line 65 - column 4, line 18 figures 1-5	
A	DE 101 32 440 A (BOSCH GMBH ROBERT) 23 January 2003 (2003-01-23) paragraphs '0001! - '0019!	1-8
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

14 July 2004

Date of mailing of the international search report

19/08/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Pöllmann, H.M.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/050217

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>DE 197 44 230 A (BOSCH GMBH ROBERT) 8 April 1999 (1999-04-08) column 1, line 1 - column 3, line 31 figure 1</p> <p>-----</p>	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/050217

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
DE 10025493	A	06-12-2001	DE 10025493 A1	06-12-2001
			WO 0189898 A1	29-11-2001
			EP 1283793 A1	19-02-2003
			JP 2003534196 T	18-11-2003
			US 2003171865 A1	11-09-2003
DE 19704841	A	13-08-1998	DE 19704841 A1	13-08-1998
			AU 6294798 A	26-08-1998
			WO 9834822 A1	13-08-1998
			EP 0958164 A1	24-11-1999
			JP 2001509754 T	24-07-2001
			US 6357839 B1	19-03-2002
DE 10132440	A	23-01-2003	DE 10132440 A1	23-01-2003
			WO 03004330 A1	16-01-2003
			EP 1406800 A1	14-04-2004
			US 2004030477 A1	12-02-2004
DE 19744230	A	08-04-1999	DE 19744230 A1	08-04-1999
			FR 2771193 A1	21-05-1999
			IT 1302575 B1	29-09-2000
			JP 11191002 A	13-07-1999
			US 2002123828 A1	05-09-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/050217

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G05B19/042 B60G17/015

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G05B B60G

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 100 25 493 A (DAIMLER CHRYSLER AG) 6. Dezember 2001 (2001-12-06) Absätze '0002! - '0022! Absätze '0042! - '0050! Abbildung 1	1-8
A	DE 197 04 841 A (ITT MFG ENTERPRISES INC) 13. August 1998 (1998-08-13) Spalte 2, Zeile 19 - Zeile 25 Spalte 2, Zeile 46 - Spalte 3, Zeile 19 Spalte 3, Zeile 65 - Spalte 4, Zeile 18 Abbildungen 1-5	
A	DE 101 32 440 A (BOSCH GMBH ROBERT) 23. Januar 2003 (2003-01-23) Absätze '0001! - '0019!	1-8
	-/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

14. Juli 2004

Absendedatum des internationalen Recherchenberichts

19/08/2004

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Pöllmann, H.M.

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 197 44 230 A (BOSCH GMBH ROBERT) 8. April 1999 (1999-04-08) Spalte 1, Zeile 1 - Spalte 3, Zeile 31 Abbildung 1 -----	1-8

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/050217

Im Recherchenbericht angeführtes Patentdokument			Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 10025493	A	06-12-2001	DE	10025493 A1	06-12-2001
			WO	0189898 A1	29-11-2001
			EP	1283793 A1	19-02-2003
			JP	2003534196 T	18-11-2003
			US	2003171865 A1	11-09-2003
DE 19704841	A	13-08-1998	DE	19704841 A1	13-08-1998
			AU	6294798 A	26-08-1998
			WO	9834822 A1	13-08-1998
			EP	0958164 A1	24-11-1999
			JP	2001509754 T	24-07-2001
DE 10132440	A	23-01-2003	US	6357839 B1	19-03-2002
			DE	10132440 A1	23-01-2003
			WO	03004330 A1	16-01-2003
			EP	1406800 A1	14-04-2004
			US	2004030477 A1	12-02-2004
DE 19744230	A	08-04-1999	DE	19744230 A1	08-04-1999
			FR	2771193 A1	21-05-1999
			IT	1302575 B1	29-09-2000
			JP	11191002 A	13-07-1999
			US	2002123828 A1	05-09-2002